Requirement Area		Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification		Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces		Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication		Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security		Approved integrity technique, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test	
Operational Environment		Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security		Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security		Module is designed to mitigate against non-invasive attacks specified in Annex “F”.			
		Documentation and effectiveness of mitigation techniques specified in Annex “F”		Mitigation testing	Mitigation testing
Security Parameter Management		Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
		Automated SSP transport or SSP agreement using approved methods			
		Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests		Pre-operational: software/firmware integrity, bypass, and critical functions test			
		Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance	**Configuration Management**	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
	Design	Module designed to allow testing of all provided security related services			
	FSM	Finite State Model			
	Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
	Testing	Functional testing		Low-level testing	
	Delivery & Operation	Initialization procedures	Delivery procedures		Operator authentication using vendor provided authentication information
	Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks		Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements